



Sibylle Berg

RCE

#RemoteCodeExecution



Glossar

AI (Artificial Intelligence) Sammelbegriff für Algorithmen, Computersysteme, Software oder Hardware, die vermeintlich intelligent ist und ganz oder teilweise autonom Entscheidungen oder Handlungen durchführen kann.

Aladdin Ein vom US-amerikanischen Finanzdienstleister BlackRock entwickeltes Datenanalysesystem, welches die Risiken von Finanzprodukten in verschiedensten Szenarien und anhand unterschiedlichster Faktoren berechnen soll.

Amper Software, welche die synthetische Erstellung von Musik und anderen Inhalten anhand von Stichworten erlaubt.

Arduino Projekt, welches quelloffene (Open-Source-)Hardware und -Software entwickelt und herstellt.

Backdoor Ein bewusst oder unbewusst offen gelassenes – jedoch meistens größtenteils unbekanntes – Einfallstor in Computersystemen, Software oder Netzwerken, mit welchem Sicherheitshürden umgangen und privilegierter Zugang erlangt werden kann.

Backend Teil eines Computersystems, der üblicherweise nicht direkt zugänglich ist. Im Backend werden oft mittels Servern, Applikationen und Datenbankdaten gespeichert und manipuliert.

Beacon Kleiner Bluetooth-Sender, der über eine Distanz von rund dreißig Metern Nachrichten an in der Nähe befindliche Endgeräte versenden kann.

Bitcoin Kryptowährung

Blockchain Dezentral organisierte Liste von kontinuierlich erweiterbaren Datensätzen, die in einzelnen Blöcken abgelegt und mittels kryptografischer Verfahren aneinandergehängt werden. Basis für Kryptowährungen oder Smart Contracts.

Bot Computerprogramm, das weitgehend automatisch Aufgaben abarbeitet, ohne auf Eingaben von menschlichen BenutzerInnen angewiesen zu sein.

Briar Freier Messenger-Dienst, der ohne zentrale Server (Peer-to-Peer-Netzwerk) auskommt und nur minimale Infrastruktur benötigt. Alle Gespräche sind verschlüsselt (End-to-End-Verschlüsselung) und können anonym (Tor) geführt werden.

Bugbot Ein Bot in der Größe und Form eines Insekts mit verschiedenen Funktionen.

Cambridge Analytica 2014 gegründetes Datenanalyse-Unternehmen, das durch die großflächige Nutzung von personalisierten Daten zur Beeinflussung potenzieller WählerInnen bekannt wurde (Mikrotargeting).

Chatbot Ein Bot, der mittels AI oder einfachen Entscheidungsbäumen automatisiert Fragen beantworten oder Konversationen führen kann.

Cloud Externes Netzwerk von Servern, Datenspeichern und Applikationen (z. B. in gigantischen Rechenzentren), welches die Nutzung von Programmen und Speicherplatz auf Abruf erlaubt.

CMBS (Commercial Mortgage-Based Securities) Eine Anleihe, welche durch Zinszahlungen von Hypotheken getragen wird. CMBS auf der Basis zweitklassiger Hypotheken (engl. subprime) spielten bei der Finanzkrise 2008 eine wesentliche Rolle.

Dieses Download-Booklet enthält das Glossar zum Hörbuch *RCE #RemoteCodeExecution* von Sibylle Berg.

Das Glossar ist der Buchausgabe entnommen: *RCE – #RemoteCodeExecution* von Sibylle Berg.

Copyright © 2022, Verlag Kiepenheuer & Witsch, Köln ® und © Argon Verlag AVE GmbH

- COBOL** 1959 entwickelte und für lange Zeit weitverbreitete Programmiersprache, optimiert für das Finanz- und Buchhaltungswesen. Noch heute bei Backend-Systemen in Banken geläufig.
- Coding** Sammelbegriff für das Programmieren und Schreiben von Software-Codes aller Art.
- Credit Score** Ein anhand unterschiedlicher Metriken und Methoden errechneter personalisierter Wert, der die Kreditwürdigkeit einer Person wiedergeben soll.
- CRISPR** Gezieltes Schneiden und Verändern von DNA (Gene Editing) mit molekularbiologischen Mitteln.
- Cryptomining** Der Prozess, mit dem Transaktionen bei unterschiedlichen Kryptowährungen in meist dezentral organisierten Netzwerken von Rechnern (sogenannte Miner) validiert werden. Das Mining ist oft ressourcenintensiv und lukrativ.
- CVE** (Common Vulnerabilities and Exposures) Referenziersystem für bekannte Schwachstellen und Anfälligkeiten von Computersystemen.
- Cyber-Defence** Der Versuch von Staaten, Unternehmen oder Privatpersonen, potenzielle Angriffe auf eigene Computersysteme vorgängig zu antizipieren und zu unterbinden.
- Cyborg** Ein Wesen, das teils organisch und teils technisch-mechanisch ist.
- Dark Pattern** Design in Apps oder Websites, das darauf abzielt, BenutzerInnen zu Handlungen zu verleiten, die ihren Interessen zuwiderlaufen.
- DDoS** (Distributed Denial of Service) Mutwillige Blockade eines Internetdienstes durch gehäufte Anfragen und Überlastung der Serverkapazitäten. Wird oft über ein Netzwerk von Bots durchgeführt. Vergleichbar in der physischen Welt mit einer Sitzblockade.
- Deepfake** Realistisch wirkende Medieninhalte – z. B. Bilder, Videos oder Audioaufnahmen –, die durch die Verwendung von AI synthetisch hergestellt oder manipuliert wurden.
- Deep Packet Inspection** Verfahren, um Datenpakete in Netzwerken zu überwachen und zu filtern. Damit lassen sich Datenströme für Zwecke der Zensur oder zur heimlichen Installation von Spyware manipulieren.
- Deplatforming** Der Ausschluss einzelner Personen oder Gruppen aus den Plattformen von sozialen Netzwerken oder anderen zentralisierten Internetdiensten.
- DevOps** Methoden zur effektiven und effizienten Zusammenarbeit zwischen EntwicklerInnen (Developers) und AdministratorInnen (Operators).
- Discord** Vor allem unter GamerInnen beliebter Onlinedienst für Sprach- und Videokonferenzen, Chats sowie Instant Messaging.
- DNS-Server** Ein Server, welcher das Domain Name System (DNS) – das »Telefonbuch« des Internets – für BenutzerInnen bereitstellt. Über das DNS wissen Rechner, unter welcher IP-Adresse eine bestimmte Website (z. B. sibylleberg.com) zu finden ist.
- DragonFlyBSD** Freies und Open-Source-Betriebssystem.
- DyRiAS** Applikation im Bereich des Predictive Policing zur vermeintlichen Risikoanalyse von Menschen in Schulen, an Arbeitsplätzen oder in Intimbeziehungen.
- Ende-zu-Ende-Verschlüsselung** Verschlüsselung von übertragenen Daten über alle Stationen hinweg. Nur die Endpunkte der Kommunikation können die Nachrichten entschlüsseln.
- FinCEN Files** Mehrere Tausend von der US-amerikanischen Anti-Geldwäsche-Behörde gesammelte Verdachtsfälle auf Geldwäsche, die im September 2020 geleakt (Leak) wurden. Sie dokumentieren verdächtige Bankgeschäfte im Umfang von 1,69 Billionen Euro.
- FinSpy** Von der britisch-deutschen Firma FinFisher GmbH entwickelte und vertriebene Spionagesoftware (Trojaner) für Smartphones und andere Endgeräte.
- Fintec** Programme und andere Technologien zur Unterstützung und Ermöglichung von Bank- und Finanzdienstleistungen.

Dieses Download-Booklet enthält das Glossar zum Hörbuch *RCE #RemoteCodeExecution* von Sibylle Berg.
 Das Glossar ist der Buchausgabe entnommen: *RCE – #RemoteCodeExecution* von Sibylle Berg.
 Copyright © 2022, Verlag Kiepenheuer & Witsch, Köln ® und © Argon Verlag AVE GmbH

- Firewall** Ein Sicherungssystem, um ein Rechnernetz oder Endgerät anhand klar definierter Regeln vor unerwünschten Zugriffen zu schützen.
- Foundry** Von Palantir entwickelte und vertriebene Software zur quantitativen Analyse großer Datenmengen.
- Freifunk** Auf WLAN basierendes Funknetz, welches von nicht kommerziellen AnbieterInnen betrieben wird. Damit lassen sich Häuser, Dörfer oder ganze Städte vernetzen.
- Frontend** Teil eines Computersystems, der üblicherweise direkt zugänglich ist. Im Frontend werden die im Backend gespeicherten und verarbeiteten Daten präsentiert.
- Gene Editing** Technik zur zielgerichteten Veränderung der DNA von Menschen, Tieren und Pflanzen z. B. anhand der CRISPR-Methode.
- Geoblocking** Regionale Sperrung von Internetinhalten durch Staaten, AnbieterInnen oder NetzwerkbetreiberInnen. Die Technik kommt insbesondere bei Filmen, Fernsehübertragungen oder Musikinhalten zum Einsatz.
- Geoengineering** Großräumiger Eingriff in die Umwelt mit technischen Mitteln – zum Beispiel zur Abbremsung der Klimaerhitzung oder zur Verringerung der Versauerung der Meere.
- Geofencing** Automatisiertes Auslösen einer Aktion (z. B. Benachrichtigung, Warnsignal oder Deaktivierung), wenn ein Endgerät einen bestimmten Bereich in Städten oder Ländern verlässt.
- GIF** Häufig animierte und als Meme verwendete kurze Bildsequenzen.
- GitHub** Zu Microsoft gehörender Dienst, der die Verwaltung, Kommentierung und Entwicklung von Software vereinfacht. Basiert auf dem Versionsverwaltungssystem Git.
- Gotham** Von Palantir entwickelte Software, welche die Suche und Ermittlung von Daten ermöglicht. Wird insbesondere von Polizei und Nachrichtendiensten zur Vernetzung unterschiedlicher Datenbanken genutzt.
- GPT-3** Durch AI getriebene und von OpenAI entwickelte Software, welche das selbstständige und synthetische Verfassen von Texten ermöglicht.
- Hackerspace** Physischer, meist offener Raum, in dem sich HackerInnen sowie an Technologie und digitaler Kunst interessierte Menschen treffen, arbeiten und austauschen.
- Hashtag** Mit einer Raute versehenes Schlagwort, das zur Vernetzung, Suche, Mobilisierung und Archivierung von Inhalten in sozialen Netzwerken genutzt wird.
- HF-Signal** Signal im Hochfrequenz-Bereich.
- Honeypot** Ein attraktiv wirkendes Scheinziel (z. B. ein Server, eine Website, eine Influencerin), das AngreiferInnen auf eine falsche Fährte oder in eine Falle locken soll.
- Implant** Ein elektronisches Gerät oder ein Schläferprogramm, das darauf abzielt, Informationen unbefugt abzufangen. Ausgewiesene Implants können auch Software nachladen, um mehr und neue Ausspähfähigkeiten zu nutzen.
- Incel** Von Misogynie geprägter cis-heterosexueller Mann, der nach Eigenaussage unfreiwillig keinen Sex hat, aber einen Anspruch auf den Körper von Frauen und ein Recht auf Sex geltend zu machen versucht.
- Internet of Bodies (IoB)** Weltweit vernetzte Sensoren und Geräte, welche vorgeblich für die eigene Gesundheit körperliche Funktionen vermessen, Daten sammeln und anderen Diensten zur Verfügung stellen. Je nach Definition ein Teilbereich oder eine Erweiterung des Internet of Things.
- Internet of Things (IoT)** Weltweite Vernetzung von virtuellen und physischen Dingen – Endgeräten, Thermostaten, Sensoren, Kühlschränken, Kameras etc. –, welche die datafizierte und digitalisierte Interaktion zwischen digitaler und physischer Welt regeln soll.
- IP-Adresse** Adresse in Computernetzwerken wie zum Beispiel dem Internet. Sie wird verwendet, um Datenpakete an die vorgesehenen EmpfängerInnen zu transportieren.

- Klickfarm** Gruppe von meist schlecht bezahlten ArbeiterInnen, die täglich stundenlang Links oder andere Inhalte im Netz auf mehreren Endgeräten anklicken. Im Gegensatz zu einem Netzwerk von Bots lassen sich solche Aktivitäten nur schwer automatisiert identifizieren und herausfiltern.
- Kryptografie** Wissenschaft der Verschlüsselung von Information (z. B. für Ende-zu-Ende-Verschlüsselung).
- Kryptowährung** Digitaler Vermögenswert wie zum Beispiel Bitcoin, der in der Regel auf einer Blockchain basiert und mittels kryptografischer Methoden Transaktionen und Vermögen dezentral erfasst, durchführt und verifiziert.
- LARP** Form des Live-Rollenspiels, bei dem die TeilnehmerInnen einen Charakter aus einer speziellen Spielwelt verkörpern und in der Gegend herumbewegen. Häufig mit aufwändiger Verkleidung und Bewaffnung, die aber nicht schmerzhaft zum Einsatz kommt.
- Leak** Nicht autorisierte Veröffentlichung – zum Beispiel von InvestigativjournalistInnen, HackerInnen oder WhistleblowerInnen – von meist geheimen Informationen. Oft auf spezifischen Plattformen wie WikiLeaks.
- Loader** Einfache Trojaner, welche die Möglichkeit bieten, aus der Distanz einen kompromittierten Computer oder Bot zu kontrollieren.
- Malware** Schadsoftware wie zum Beispiel Viren oder Trojaner, welche mit der Absicht entwickelt wurden, beim Opfer unerwünschte oder schädliche Funktionen auszuführen. Werden oft in vermeintlich unproblematischer Software versteckt oder heimlich eingeschleust und verbreitet sich mitunter selbstständig weiter.
- Man-in-the-Middle** Eine Angriffsform auf Computernetze, bei der sich jemand zwischen zwei KommunikationspartnerInnen einschleust und dadurch die vollständige Kontrolle über den Datenverkehr hat.
- Maschinelles Lernen** (Machine Learning) Form der algorithmischen Generierung von vermeintlichem Wissen (AI). Dabei lernen Systeme durch statistische Methoden und auf der Basis von Trainingsdaten Muster und Gesetzmäßigkeiten und können diese in anderen Daten, die sie nicht als Lernmaterial hatten, wiederum erkennen.
- Meme** In der Regel humoristische, satirische oder gesellschaftskritische Bilder, Videos, Zeichnungen, Inhaltsformen etc., die sich übers Internet oftmals viral unter Menschen verbreiten.
- Metadaten** Strukturierte Daten, welche Informationen (z. B. Aufnahmedatum, GPS-Koordinaten, Lautstärke) über andere Daten enthalten.
- Mikrotargeting** Kommunikationsstrategie – insbesondere im Marketing und politischer Propaganda –, bei welcher feinkörnige Zielgruppen mit passgenau zugeschnittenen Inhalten bespielt werden. Dafür werden die Präferenzen und Interessen sowie das Verhalten von Menschen sowie die Beziehungsnetze zwischen Menschen möglichst vollständig erfasst.
- MixNet** Ein Netzwerk, in dem die Kommunikation durch das Umleiten über mehrere Zwischenstationen (sogenannte Mixe) anonymisiert wird.
- Nanobot** Hypothetische, autonome Bots im Kleinstformat z. B. für medizinische Zwecke, zur Produktion neuer Rohstoffe oder zur Überwachung und Spionage.
- Nanotechnologie** 1959 hielt der Physiker Richard Feynman auf einer Tagung der American Physical Society einen Vortrag mit dem Titel »There's Plenty of Room at the Bottom«. Darin erörterte er einen zukünftigen Prozess, bei dem Wissenschaftler einzelne Atome und Moleküle manipulieren könnten, um einzigartige Eigenschaften in Materialien zu schaffen. Dieses Konzept wurde ein Jahrzehnt später von Professor Norio Taniguchi als »Nanotechnologie« bezeichnet.
- Nanorobotik** **Nanobot**
- Neuralink** Von Elon Musk mitgegründetes Neurotechnologie-Unternehmen, das versucht, eine Schnittstelle zwischen Gehirnen und Computern zu entwickeln und herzustellen.
- NFT** (Non-Fungible Token) Ein auf der Blockchain aufgebautes digital geschütztes Objekt, das dessen vermeintliche Einzigartigkeit im digitalen Raum festhält. Wird vor allem für Finanzspekulation und die ökonomische Verwertung digitaler Kunst oder Memes verwendet.

Dieses Download-Booklet enthält das Glossar zum Hörbuch *RCE #RemoteCodeExecution* von Sibylle Berg.
 Das Glossar ist der Buchausgabe entnommen: *RCE – #RemoteCodeExecution* von Sibylle Berg.
 Copyright © 2022, Verlag Kiepenheuer & Witsch, Köln ® und © Argon Verlag AVE GmbH

NSO Group Israelisches Unternehmen, das Spionagesoftware wie Trojaner (insbesondere Pegasus) für Staaten, Polizei und Geheimdienste entwickelt.

Nudging Methode, um das Verhalten von Menschen mittels subtiler Hinweise, Farbpsychologie oder perfiden Designentscheidungen unerkannt zu beeinflussen.

OCEAN Weitverbreitetes Standardmodell der Persönlichkeitspsychologie, in welchem Menschen anhand von fünf Skalen (openness/Offenheit, conscientiousness/Gewissenhaftigkeit, extraversion/Extraversion, agreeableness/Verträglichkeit und neuroticism/Neurotizismus) eingeordnet werden.

Octagon In der Schweiz entwickeltes, angewandtes und wissenschaftlich nicht unabhängig validiertes Prognostikwerkzeug (Predictive Policing), um die Gewaltbereitschaft einer Person anhand von acht Dimensionen zu bestimmen.

OpenBSD Freies und Open-Source-Betriebssystem mit Fokus auf Sicherheit.

Open-Source Hardware oder Software mit öffentlichem Quellcode oder Bauplan.

OpenSSL Freie Software, mit welcher die Kommunikation in Computernetzwerken verschlüsselt und vor Lauschangriffen geschützt werden kann.

PAIP (Police Applications Intercommunications Protocol) In Deutschland weitgehend geheim operierendes Ortungssystem, um Menschen, Fahrzeuge und Waren zu orten und zu verfolgen.

Palantir US-amerikanisches Unternehmen, welches sich auf die Analyse von großen Datenmengen spezialisiert. Bekannt durch die Zusammenarbeit mit Anti-Terror-Behörden (Gotham) und als Dienstleister von Banken und Hedgefonds (Foundry).

Parler Alternatives soziales Netzwerk für Mikroblogging. Wird vor allem von rechtslibertären, rassistischen und verschwörungsideologischen Männern verwendet.

Patreon Plattform, welche die Crowdfinanzierung von KünstlerInnen, AutorInnen, MusikerInnen etc. durch regelmäßige Spenden ermöglicht.

Payload Der Teil einer Schadsoftware, welcher die bösartige Aktion ausführt.

Peer-to-Peer-Netzwerk (P2P) Netzwerk aus gleichberechtigten Rechnern (sogenannte Peers), die unabhängig voneinander mit allen anderen kommunizieren und Daten austauschen können.

Pegasus Von der NSO Group entwickelter Trojaner, der Smartphones überwacht und unter anderem für die staatliche Spionage von Oppositionellen und JournalistInnen verwendet wird.

Precobs Predictive Policing Software, welche versucht, Einbrüche und andere Vorkommnisse anhand von statistischen und psychologischen Modellen vorherzusagen (z. B. mit dem Near-Repeat-Ansatz, der annimmt, dass Einbruchserien gewissen Mustern folgen).

Predictive Policing Versuch, mit algorithmischen Methoden und der Analyse vergangener Verbrechen zukünftige Straftaten zu verhindern oder den Einsatz von Polizeikräften zu optimieren.

Proxy Vermittlungsrechner in einem Netzwerk, der Anfragen annimmt und an das beabsichtigte Ziel weiterleitet. Durch diese Zwischenstufe kann die Kommunikation ein Stück weit anonymisiert werden.

Quantencomputer Computer, der durch die Verwendung von quantenmechanischen Prinzipien über bedeutend mehr Rechenleistung verfügt als herkömmliche Computer auf elektrischer Basis. Dadurch ließe sich auch klassische Verschlüsselung mit »brute force« umgehen, was sich wiederum mit Quantenverschlüsselung umgehen ließe.

Rack Oft standardisierte Gestelle in Rechenzentren, in welchen die Rechner verstaut und vernetzt sind.

Ransomware Ein Trojaner, der Daten auf dem infizierten System verschlüsselt und vorgeblich nur gegen Lösegeld wieder freigibt.

Raspberry Pi Einfacher, günstiger und kleiner Computer in der Größe einer Kreditkarte, der sich durch hohe Anpassbarkeit auszeichnet.

Dieses Download-Booklet enthält das Glossar zum Hörbuch *RCE #RemoteCodeExecution* von Sibylle Berg. Das Glossar ist der Buchausgabe entnommen: *RCE – #RemoteCodeExecution* von Sibylle Berg. Copyright © 2022, Verlag Kiepenheuer & Witsch, Köln ® und © Argon Verlag AVE GmbH

- RCE** (Remote Code Execution) Angriff, bei welchem die angreifende Person oder Organisation aus der Distanz Befehle im Zielsystem ausführen kann.
- Reddit** Internetforum, das zu den zwanzig am häufigsten besuchten Websites der Welt gehört.
- RF-Detektoren** Geräte, welche Radiowellen in Netzwerken aufspüren (zum Beispiel, um versteckte Wanzen oder Kameras zu entdecken).
- RFID** Technologie für die automatische und berührungslose Identifikation von Objekten (z. B. Endgeräten, Kreditkarten, Identitätskarten) über Radiowellen.
- Router** Physische Netzwerkgeräte, welche Datenpakete weiterleiten können und meist zur Internetanbindung genutzt werden.
- Sentiment-Analyse** Algorithmische Methode zur automatisierten Erkennung der Stimmung (Haltung, Emotionen, Werte etc.) in Texten und anderen Medien.
- Server** Gerät, das über ein Netzwerk Dienstleistungen, Daten oder Programme für andere Computer (sogenannte Clients) zur Verfügung stellt.
- Signal** Messaging-Dienst, welcher ausschließlich auf Open-Source und Ende-zu-Ende-Verschlüsselung setzt und kaum Daten über die BenutzerInnen zentral speichert. Die Nachrichten werden allerdings über einen zentralistischen Dienst vermittelt, der somit anfällig für DDoS ist.
- Smart Contract** Programm, welches über eine Blockchain automatisiert Verträge ausführt und durchsetzt.
- Smartmeter** Ressourcenzähler (z. B. Gas, Strom, Wasser), welche digital Daten über den Verbrauch oder den Tarif empfangen und weiterleiten können.
- Social Bot** Bots, welche vor allem in sozialen Netzwerken automatisiert Antworten geben oder regelgeleitet Informationen wiedergeben.
- Social Freezing** Das vorsorgliche Einfrieren von Eizellen ohne medizinischen Grund – meist um die Reproduktionsfähigkeit zu einem späteren, als ideal angesehenen Grund zu gewährleisten.
- SolarWinds** IT-Firma, in deren Update-Prozess HackerInnen Malware versteckt hatten, mit denen sich die KundInnen ausspionieren ließen. Die USA waren von diesen Supply-Chain-Angriffen im schwersten Maße betroffen.
- Sounding** Stimulation der Harnröhre mit verschiedenen Werkzeugen.
- Telegram** In Russland entwickelter und vor allem in rechtslibertären und verschwörungsideologischen Kreisen weitverbreiteter Messaging-Dienst. Über öffentliche Gruppen können auch Funktionen von anderen sozialen Netzwerken übernommen werden. Telegram betreibt – ähnlich wie Signal – eine zentralistische Infrastruktur, allerdings mit starker Verteilung und vielen Serverstandorten.
- Terminal** Schnittstelle zur Eingabe und Anzeige von Daten sowie zur Ausführung von Befehlen in Computernetzwerken.
- Threema** In der Schweiz entwickelter und beheimateter Messaging-Dienst, der auf Privatsphäre mittels Ende-zu-Ende-Verschlüsselung setzt. Threema betreibt ähnlich wie Signal eine zentralisierte Infrastruktur, die somit vor DDoS-Angriffen nicht gefeit ist.
- TKÜ** (Telekommunikationsüberwachung) **Vorratsdatenspeicherung**
- Tor** Netzwerk, welches die Verbindungsdaten wirksam anonymisiert. Es schützt die NutzerInnen vor der Überwachung, Zensur und Analyse des Datenverkehrs im Internet.
- Torrent** Protokoll für den kollaborativen, dezentralen und schnellen Austausch von großen Datenmengen in kleinen Einheiten über ein Peer-to-Peer-Netzwerk.
- Transponderbeacon** »Beacon« bedeutet übersetzt »Funkbake« und bezeichnet im ursprünglichen Sinne einen Sender-Empfänger, der automatisch ein Signal aussendet, wenn er von einem Radar erfasst wird. Das Signal wiederum erscheint auf dem Display des Radars und liefert Informationen über Entfernung und Identifizierung (beispielsweise von Bojen). Ist heute die Rede von »Beacons«, sind aber in der Regel kleine Bluetooth-Sender, Statusnachrichten in einem WLAN o. ä. gemeint. Der Effekt ist aber vergleichbar.

Dieses Download-Booklet enthält das Glossar zum Hörbuch *RCE #RemoteCodeExecution* von Sibylle Berg.
 Das Glossar ist der Buchausgabe entnommen: *RCE – #RemoteCodeExecution* von Sibylle Berg.
 Copyright © 2022, Verlag Kiepenheuer & Witsch, Köln ® und © Argon Verlag AVE GmbH

Trojaner Schadprogramm, welches als nützliche Anwendung getarnt, aber im Hintergrund unwissentlich andere Funktionen – meist zur Überwachung oder externen Steuerung (RCE) – ausführt.

Trollfarm Gruppen von Individuen, die zum Beispiel im geheimen staatlichen Auftrag verdeckt politische Propaganda mittels falscher Identitäten verbreitet.

Twitch Weitverbreitete und vor allem bei GamerInnen beliebte Live-Streaming-Plattform.

Verschlüsselung Kryptografie

Vorratsdatenspeicherung Verpflichtung von Kommunikationsanbietern zur Speicherung und Weitergabe bestimmter Daten, welche von diesen für die Bereitstellung der Dienstleistung erhoben werden. Die Daten werden für die Verfolgung von Straftaten von Polizeien und Geheimdiensten eingefordert.

VPN (Virtual Private Network) Netzwerkverbindung, mit welcher ein privates Netz in den öffentlichen Raum erweitert wird. Damit lassen sich Daten über den öffentlichen Raum so miteinander austauschen, als ob die Geräte mit dem privaten Netz verbunden wären.

White Hat HackerIn, welche ihre Fähigkeiten und ihr Wissen gesetzesgetreu und gemäß der Prinzipien der Hackerethik anwendet. Im Gegenzug dazu Black Hats, die mit krimineller Energie – auch im Auftrag von Regierungen oder Organisationen – handeln. Dazwischen wird auch der Grey Hat unterschieden, der Gesetzesübertretungen machen mag, allerdings zu nicht monetären, gesellschaftlichen und politischen Zwecken (auch: Hacktivismus).

WikiLeaks Leak

Wirecard Bis 2020 existierender deutscher Finanzdienstleister, bei dem bekannt wurde, dass 1,9 Milliarden Euro »fehlten«.

Wordpress Freie und Open-Source-Software, um Informationen und Inhalte im Internet anzuzeigen und zu bewirtschaften. Rund 30 Prozent der Websites nutzen Wordpress, das durch die einfache Erweiterbarkeit und Anpassbarkeit oft diverse Einfallstore für Malware, RCE oder andere Angriffe bietet.